NSA review completed

1. DIA, NSA, and CIA ("the big three") are to establish a program of computer security certification for all Intelligence Community members. CIA would be required to perform detailed technical evaluations of Department of State, Department of Energy, etc., systems.

Points Supporting: Certification by the "big three" will allow for enhanced consistency and technology sharing throughout the Intelligence Community.

Points Opposing: Technical evaluations to the degree required for certification take from 4 to 24 months each. ISSD currently has insufficient resources to certify Agency systems including CIA contractors, and will not have sufficient resources to provide these services to other NFIB members even with the projected out-year growth. The DCID applies to all systems which process classified information, not just those processing Sensitive Compartmented Information. The number of non-CIA, non-DoD systems processing classified information is estimated to be greater than one thousand. This certification responsibility would severely detract from the primary mission of ISSD. The Department of State also emphatically objects to this provision of the DCID. This issue is related to issues 2 and 4.

ISSD Position: Oppose the issue. Certification should be the responsibility of each NFIB member.

2. The DCID requires that several annual reports be forwarded to the ICS concerning the security posture of all systems under the cognizance of each NFIB member.

Points Supporting: The ICS will be in the best position to oversee implementation of the DCID through annual status reporting. These annual status reports will be a major input to the Community THREAT paper which is published annually under the DCI COMPUSEC program.

Points Opposing: The DCID applies to all systems which process intelligence information, not just those which process Sensitive Compartmented Information. The reporting requirement

DIA Review Completed.

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

25X1

includes a very large number of systems. Record keeping and accounting are very important, but such requirements should not be allowed to detract from the primary mission of ISSD. Data calls are very time consuming and resource driven. CIA has been reluctant, in the past, to provide total numbers of classified systems to other Federal agencies. DIA has objected to report writing on the grounds that it would detract from the primary mission and support provided to its customers. This issue is strongly related to issue 1 (which gives CIA responsibility for reporting on all non-DoD, non-CIA systems processing classified information, and issue 4 requiring CIA to keep records for the same systems).

ISSD Position: Oppose the issue. Call for a single annual status report on the status of computer security by each NFIB member.

3. DIA, NSA, and CIA are to establish media release and destruction centers to service all intelligence organizations throughout the world. In this joint program, CIA, NSA, and DIA are required to coordinate to ensure that a local center is available.

Points Supporting: By placing responsibility for media destruction with the "big three" and establishing destruction centers throughout the world, a valuable consistent destruction capability will be made available to the entire Community. This will reduce problems encountered in inadvertent release of intelligence information in waste products.

Points Opposing: It is possible, under this program, that NSA or DIA would be responsible for destruction of media containing extremely sensitive CIA data. ISSD finds this proposal to be unacceptable to CIA. We believe that NSA/DDO will voice the same objection based upon their strict adherence to need-to-know. It is also possible, under this program, that NSA, DIA, and CIA would each have co-located centers throughout the world. Establishment of numerous (more than 10) media destruction and release centers would severely tax valuable CIA resources and would provide a small set of vulnerable operations subject to attack through hostile intelligence infiltration. Currently, each CRAFT site handles media destruction and release -- we consider this procedure effective and secure.

ISSD Position: Oppose the issue. Each NFIB member should be responsible for destruction and control of its classified materials. Recommend that the DCID provide a media destruction standard which all NFIB members would follow.

4. NSA and DIA are to keep accreditation records for all DoD components which process intelligence information. CIA is to keep records for all non-DoD components which process intelligence information.

Points Supporting: Since the ICS is to oversee implementation of computer security for the Intelligence Community, it is best that "the big three" be used as a central repository and reference source to determine the status and requirements for security. Through "centralized" record keeping, status information will be more readily available to the ICS so that the ICS can carry out its oversight responsibility efficiently.

Points Opposing: In the past, CIA has been reluctant to provide total numbers of systems (e.g., communications and computer) to other Federal agencies (OMB and NSA) which collect such information. NSA has also been opposed to providing such information. DIA has been opposed to reporting for reporting's sake as detrimental to its ability to provide security evaluation services to its customers. The Department of State also objects to this provision of the DCID. This "centralized" record keeping responsibility would be a large burden and would detract from the primary mission of ISSD. There are nine NFIB members, each most capable of keeping records of their own systems, and who are most cognizant of the status of systems within their purview. It seems unreasonable, and an unneeded burden on CIA, to reduce the number of record repositories to three vis-a-vis nine. Furthermore, the ICS has no responsibility for oversight of these Senior Intelligence Officers. This issue is related to issues 1 and 2.

ISSD Position: Oppose "big three" record keeping.

5. Multi-Level Mode of Operation is defined by which users with a SECRET clearance would have access to systems which process SCI.

Points Supporting: The intent of multi-level mode is to support Tactical US Forces operating at the SECRET security

level. Furthermore, relations with NATO and foreign governments require interchange of information, based upon current intelligence, for U.S. national security. Several Community systems are currently operating in the multi-level security mode, due to operational necessity, even though such operation is not permitted. These systems should be reaccredited for the multi-level mode of operation.

Points Opposing: The DCID permits, in addition to Tactical US Force access, access by Foreign Tactical Forces (e.g., NATO, ROK). In the case that Foreign Tactical (or Strategic) Forces have access, it is ISSD's position that all information related to collection sources and methods (including technical and human) must be excluded from the system. Human and technical collection resources are too valuable and sensitive to permit a chance of compromise to Foreign forces. CIA has not objected to presence of product-oriented compartments in multi-level systems. DCID 1/19 also provides a provision for enhanced protection of collection-oriented compartments vis-a-vis product-oriented compartments.

ISSD Position: Support the issue, but amend the definition of multi-level mode to exclude information related to intelligence collection sources and methods.

6. The ICS will oversee the implementation of the DCID by NFIB members.

Points Supporting: Through centralized oversight, the ICS will be the single point of authority for DCID interpretation. This single point of authority will lead to consistency (and interoperability) of programs among the NFIB members, and will provide a single point of authority for resolution of disputes among the NFIB members. Consistent implementation and interpretation of the DCID is necessary in order to achieve compatibility and interoperability across the Intelligence Community. This will lead to enhanced data sharing.

Points Opposing: This provision insults the integrity, abilities, and perogative of NFIB members. Centralization of oversight provides for no enhancement of security, it may actually reduce security by removing perogative from the persons who are closest to the problem. Each NFIB member is capable of overseeing, and in the best position to oversee,

their own security program. NFIB members are capable of settling their own disputes. Oversight is a role not traditionally associated with the ICS. The ICS has traditionally had a facilitation and coordination role. NFIB members are Senior Intelligence Community Officials and do not need oversight by the ICS.

ISSD Position: Oppose the issue.

7. The DCID provides a standard for security labeling of data within computer systems and their associated magnetic media. Along with this standard is an implied processing mechanism.

Points Supporting: Through implementation of a single, consistent standard for labeling and label processing within computer systems, compatibility and interoperability can be more readily achieved. Compatibility and interoperability of labeling will enhance the ability (timeliness, format, etc.) to share information among NFIB members.

Points Opposing: ISSD has taken the lead for the Community in development of a standard for labeling of data held within computer systems. The DCID is not entirely consistent with the direction being set by ISSD. The DCID view of labeling also is inconsistent with the view of the National Computer Security Center. The ramifications of acceptance of the DCID standard are that the DCID may set a labeling and label processing standard which:

(a) does not meet CIA requirements; and,

(b) is incompatible with the products which vendors are actively building under the National Computer Security Center program.

ISSD Position: Support the development of a labeling standard. Oppose the particular standard presented in the Draft DCID until a full NFIB member review and concurrence has been accomplished.

8. The DCID defines standard mechanisms and solutions for AUTODIN security problems.

Points Supporting: AUTODIN is an old (circa 1970) record communications system which is critical to the Department of Defense for communications and exchange of product reports. AUTODIN cannot be replaced in the near term, so its security capabilities must be enhanced through standardization of interfaces to it. The DoD NFIB members have not been able to agree on a single standard for interface to AUTODIN; therefore, the DCID should resolve the issue.

Points Opposing: The DCID has traditionally been a high-level policy document, but the current draft provides specific mechanisms which address particular problems in DoD. We consider definition of particular mechanisms to be inappropriate subject matter for a high-level policy document. Additionally, the mechanisms proposed in the DCID (for AUTODIN) do not effectively solve the AUTODIN problems, they simply provide a measure of integrity which is not currently implemented. NSA has opposed the proposed mechanisms; DIA has supported them.

ISSD Position: A standard for this vulnerable system is needed, but that standard should not be set in a high-level document such as the DCID. The NFIB members who use and accredit AUTODIN interfaces should agree on standards for its use.